UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

DAVID HOUSE, Plaintiff, v. JANET NAPOLITANO, in her official capacity as Secretary of the U.S. Department of Homeland Security; ALAN BERSIN, in his official capacity as Commissioner, U.S. Customs and Border Protection; JOHN T. MORTON, in his official capacity as Director, U.S. Immigration and Customs Enforcement, Defendants.	)	Civil Action No. 11-10852-DJC

DECLARATION OF ALEXANDER STAMOS

I, ALEXANDER STAMOS, hereby declare the following:

1. I have been retained by counsel for David House to analyze the government's justifications for the length of time it took to make verified forensic copies of Mr. House's electronic devices.

Background and Qualifications

2. I am a co-founder of iSEC Partners ("iSEC") and currently serve as its Vice President and the Chief Technical Officer. iSEC is an information security consulting firm headquartered in San Francisco, with offices in Seattle and New York and is a fully owned subsidiary of the NCC Group plc, headquartered in Manchester, UK. Our work includes software assurance, infrastructure penetration testing, code review, incident response and forensics. Our clients

include Microsoft, Oracle, eBay, McKesson, Salesforce.com, Google, Autodesk, Charles Schwab, JPMorgan Chase, Bank of America, Wells Fargo, ING Direct and Motorola.

3. Before founding iSEC Partners I worked as a Managing Security Consultant with the security consultancy @stake, and I was the security lead at Loudcloud, a managed hosting provider. I have also worked for the EO Lawrence Berkeley National Laboratory. I hold a BS in Electrical Engineering and Computer Science from the University of California, Berkeley, where my studies included graduate classes in networking and computer security. I was awarded a Certified Information Systems Security Professional (CISSP) certification in April 2003. I am a frequent speaker at leading security and technology conferences, such as Black Hat USA, CanSecWest, Microsoft BlueHat, the Web 2.0 Expo, CTIA, OWASP App Sec, and the FinancialServices Information Sharing and Analysis Center (FS-ISAC). I have also spoken on the topic of computer forensics to private audiences at the FBI's Regional Computer Forensics Laboratory, and the Federal Reserve Banks in New York and Boston.

4. Over the last six years I have been retained as an expert witness in seven separate civil litigation matters and performed as the technical lead for dozens of forensics and incident response projects. My forensics work includes investigations for Charles Schwab, Autodesk, Facebook and The Davidson Companies.

5. A copy of my resume is attached to this report.

Topic of Report

6. I have been asked to review the declaration of Robert Marten and to provide an opinion on whether the reasons set forth in paragraphs 10-12 of the declaration justify the extended period during which the devices were detained to make verified forensic copies. In my opinion, the process of imaging and verification described in the declaration should not have taken more

than 18 hours and did not require the one week period that the devices were retained by ICE in Chicago and certainly did not require the period of nearly six weeks that the devices were retained in New York.

Overview of the Process of Computer Forensics

7. Computer forensics is the use of scientific and technical means to determine what actions have been undertaken by users, software and remote attackers on a computing system. Computer forensics is mostly concerned with finding and analyzing the stored data on a computing system, also known as state. Examples of components that store state that can be examined during the forensics process include the system's hard disk drive, a solid state drive, external drives (such as Flash drives), optical media (such as burned compact discs) and the various types of system RAM.

8. Computer forensics is generally broken down into two broad categories, analysis of "live" and "dead" systems. Live systems are computers that are still running and therefore have retained state in the volatile Random Access Memory (RAM) of the system. RAM is used as scratch space for the operating system and running programs, and is generally not accessible to the end-user in the same way that the system's hard drives or external disks are via graphical interfaces like the Windows Explorer. Since it is very difficult to access the running system's RAM without causing changes to the evidence being gathered, the majority of forensics projects fall under the "dead" category, and live forensics is generally reserved for incident response investigations involving new malware or machines that are under active control by an attacker. Neither of those situations apply here, and since Marten does not give any indication that the system's RAM was imaged I will assume that ICE was performing dead system forensics per forensic best practice through the rest of this declaration.

9. The vast majority of forensically useful data from a laptop computer is contained on the laptop's hard drive, and although there are other types of state that can be collected by a forensic examiner there is no indication that anything other than the hard drive was of interest to Marten. I am using the term hard drive generically to include implementations that do not use a spinning metal disc, such as a solid-state drive (SSD). SSDs are functionally equivalent to traditional hard drives in almost all respects relevant to forensic examination.

10. As Marten explains in paragraph 7 of his declaration, it is generally considered best practice for a forensic examiner to make an identical bit-for-bit copy of a hard drive, verify that the copy is correct and to perform his investigation on the copy. The normal use of an operating system irrevocably changes the state of the hard drive in dozens of ways so forensic examiners generally never boot the target system during their investigation, instead they use one of four methods to image the hard drive in a way where they can prove that no changes to the hard drive occurred.

11. The first method is to remove the system's hard drive and connect it to a hardware write-blocker. These are specialized devices that interface with the target hard drive using the drive's native protocol (usually SATA) on one side and provide a more generic interface to the examiner's system on the other (such as USB or Firewire). The hardware write-blocker uses specialized logic to relay commands to read data from the drive but not commands to write data, and the use of these products is generally considered by forensic examiners as the easiest and safest way to capture a target drive. Equivalent technology also exists for safely reading USB flash drives as well as memory formats common to digitals cameras, such as compact flash (CF) and secure digital (SD). The speed of this technique is generally limited by the connection type used between the hardware write-blocker and the examiner's system.

12. The second method is to use software write-blocking. In this scenario, the examiner loads a specialized software product on his system that prevents the operating system from relaying write commands to the target device. This is generally considered an inferior solution, since software write-blockers are known to fail in ways that are difficult to detect and cannot block write commands issued by the underlying hardware. A popular commercial product that provides this kind of blocking is EnCase Forensic Edition.

13. The third method is the use of a high-speed forensics disk duplicator. This is a specialized piece of hardware that can operate without a connected computer system and which makes a verified copy of a hard drive onto another physical drive. This technique is often used for capture of hard drives in the field, since it can be much faster than other techniques and is generally only limited by the speed of the hard drive itself.

14. The fourth method is to boot an alternate operating system on the target system and to stream the system's hard drive across a network connection to the examiner's workstation. This is considered a more risky option, since a mistake by the examiner could lead to the target system booting into its standard operating system and modifying the disk. This technique is most useful when imaging data from computer servers with large or complicated disk arrays, which is not applicable to Mr. House's laptop.

15. All four of these techniques should be able to image a normal laptop hard drive in less than 12 hours, baring a serious hardware failure or rare types of hardware encryption. Marten mentioned neither a failure or hardware encryption mechanism in his declaration.

16. After a target disk is imaged using one of these methods it is then considered best practice to verify the accuracy of the copy by calculating a cryptographic hash of the drive and the copy. A cryptographic hash is a mathematical mechanism for generating a small fingerprint

from an arbitrarily large amount of data and can be used to detect any modification of forensic data during the examination process. Currently SHA1 is considered the best algorithm for calculating this fingerprint, although the older and less secure MD5 function is also often used for compatibility reasons. A proper cryptographic verification will read the target disk a second time to insure that no errors were inserted into the data stream during the copying process.

17. A wide variety of free and commercial software tools are available to perform the imaging, verification and examination of hard drives and external storage. Popular commercial products include Guidance Software's EnCase suite and AccessData Forensic Tool Kit (FTK). Popular free tools include dcfldd and The Sleuth Kit (TSK).

18. Forensic tools are able to access data that is not readily available during the normal operation of a computer system, including deleted, hidden and temporary files. This is another reason why it is important for a forensic examiner to make an exact copy of the target drive and to examine that copy on a separate workstation with special tools instead of booting the machine and viewing files via the operating system.

Creating Verified Forensic Copies of Mr. House's Electronic Devices

19. Marten ascribes the delay solely to problems in the making of two verified forensic copies of the data contained in Mr. House's computer. He identifies no factors explaining delay in the forensic examination of the flash drive and digital camera other than the issues of personnel and workload.

20. With regards to the lack of knowledge of a password, this should not affect the ability to make a verified forensic copy of the data or increase the amount of time necessary to do so. The standard forensic imaging process utilizes a method of copying the drive external to the system's normal operating system, and access to the user's password is completely irrelevant to any of the

four imaging methods I described previously. After the drive is imaged it is also not necessary to use a password to examine files on the disk, these files would be easily found and viewed by any of the tools I named previously. The only situation where a password is required to access data on a hard drive would be the use of disk or file encryption, and Marten makes no reference to those technologies being used by Mr. House.

21. With regards to having two operating systems, the partition of a computer's hard drive and the use of a dual boot system employing different operating systems on a single computer is not "non-standard" and is not unusual. For example, Apple provides a supported mechanism for dual booting modern Macintosh computers called Boot Camp, and dozens of tools to facilitate dual booting on PCs are available. The Linux operating system is widely used. A properly trained and certified computer forensic technician would be familiar with the Linux operating system and with dual boot systems. Having two operating systems does not increase the time required to copy the data. A forensic capture of a hard drive collects the entire drive and the speed at which this happens is independent of the contents of the drive. Forensically imaging a blank hard drive generally takes the same amount of time as one that is full of data. Likewise, all of the major free and commercial forensics products support examining hard drives with multiple operating systems, and all of them support the common Linux filesystem types. In a product such as EnCase or FTK, there would be no additional work necessary to capture and view the contents of a hard drive containing both Windows and Linux, although some examination steps after the initial imaging might need to be repeated for each OS.

22. In paragraph 12, Marten states that "Third, a separate computer had to be set up with forensic software to see if the images on Mr. House's devices had been made correctly. This set-up also took time and also required the time of an ICE computer forensics agent. ICE could only

return Mr. House's devices to him after the images had been verified on the reviewing computer as correct and accurate copies." In my opinion this should not have caused a delay, since the verification step should have been performed during the initial capture of the hard drive and does not require any additional software. Some groups consider it best practice to build a new forensics workstation for each project, but this step can be automated to occur very quickly and, at worst, should take about four hours of time to install a new operating system and a forensics software package.

I declare under penalty of perjury that the foregoing is true to the best of my knowledge, information and belief.

Alexander Stamos

Date: November 21, 2011